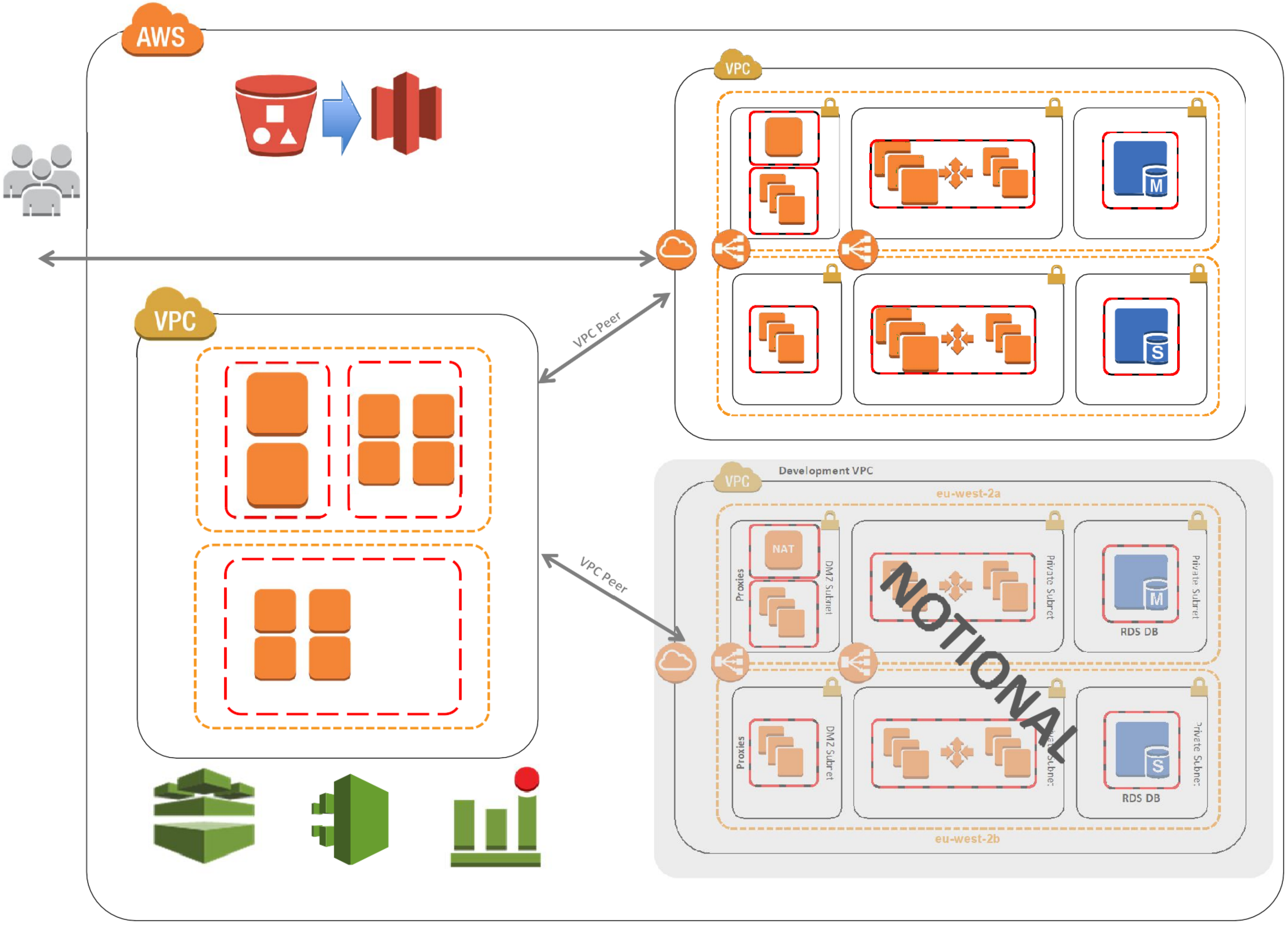
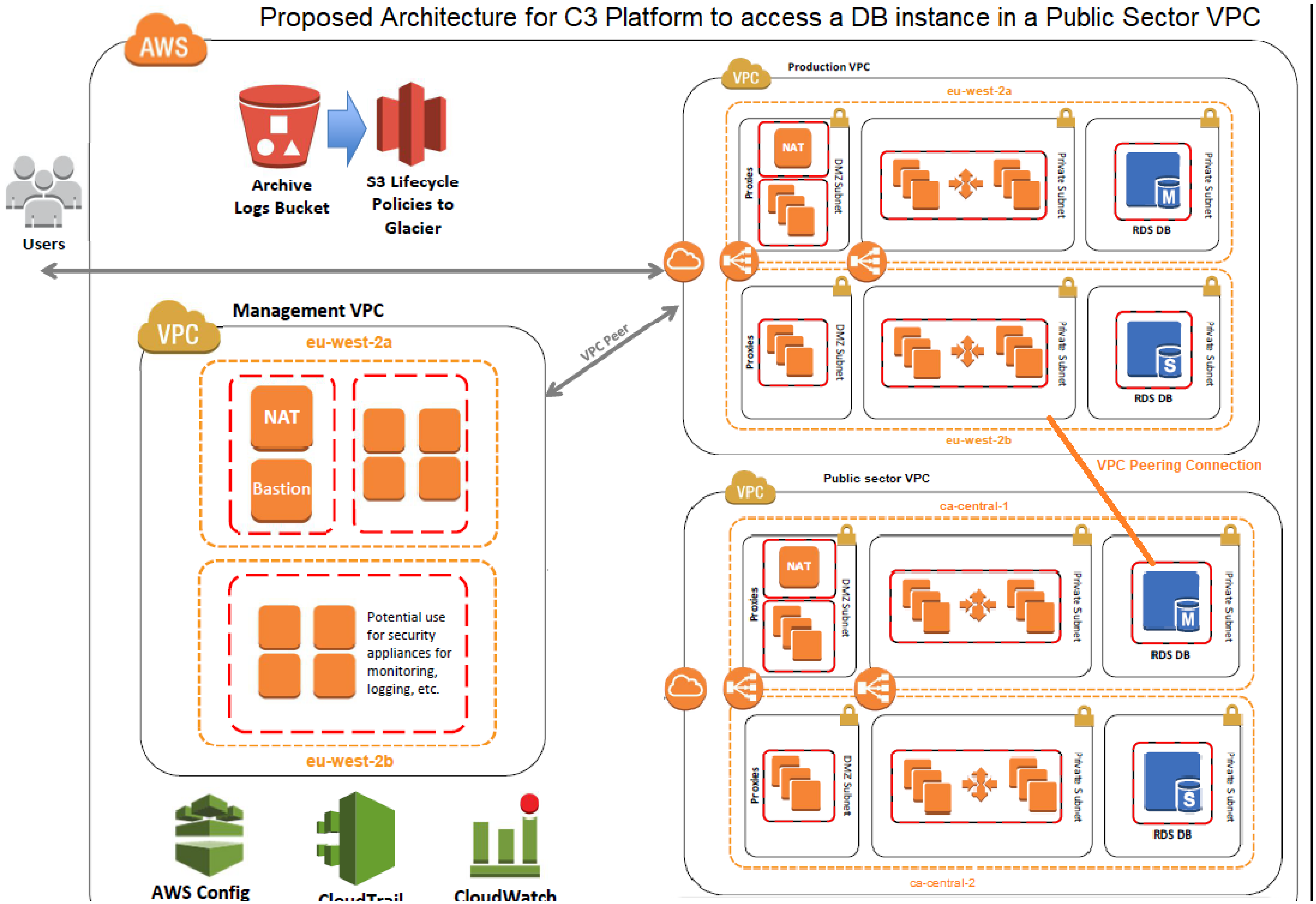
Scenario 1 – Current

C3 Architecture with Production, Management & Notional VPCs and Managed RDS



- Basic AWS Identity and Access Management (IAM) configuration with custom (IAM) policies, with associated groups, roles, and instance profiles
- Standard, external-facing Amazon Virtual Private Cloud (Amazon VPC) Multi-AZ architecture with separate subnets for different application tiers and private (back- end) subnets for application and database
- Amazon Simple Storage Service (Amazon S3) buckets for encrypted web content, logging, and backup data
- Standard Amazon VPC security groups for Amazon Elastic Compute Cloud (Amazon EC2) instances and load balancers used in the C3 application stack
- Three-tier Linux web application using Amazon EC2 Auto Scaling and Elastic Load Balancing, which can be modified and/or bootstrapped with customer application
- A secured bastion login host to facilitate command-line Secure Shell (SSH) access to Amazon EC2 instances for troubleshooting and systems administration activities
- Encrypted, Multi-AZ Amazon Relational Database Service (Amazon RDS) MySQL database
- Logging, monitoring, and alerts using AWS CloudTrail, Amazon CloudWatch, and AWS Config rules
- Encrypted secondary EBS volumes on all EC2 instances

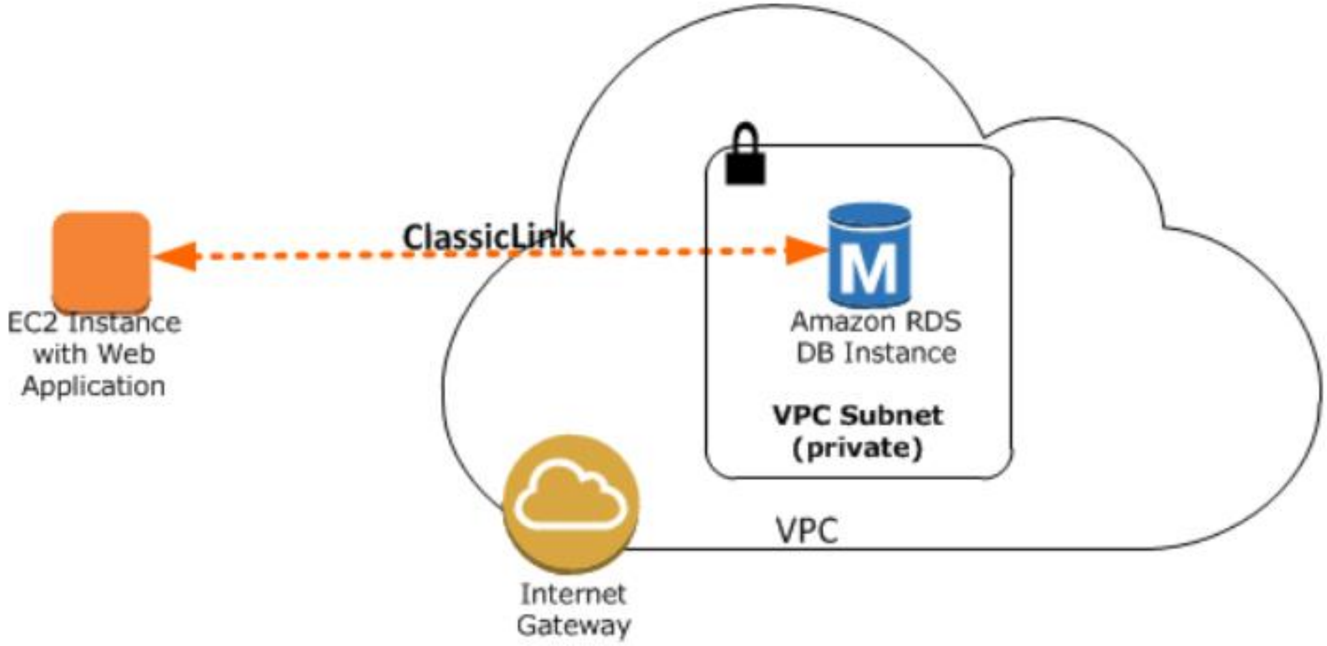
Scenario 2 - Proposed



- Basic configuration as Scenario 1
- A VPC Peering connection is proposed in this scenario, where instances in the C3 VPC instance can communicate with the Public Sector VPC in a different Region.
- The Application instances will be hosted in the C3 VPC, and the RDS instance will be in the Public Sector VPC.
- The Application will have to be configured to make API calls to the Public Sector RDS DB instance to read and write data.
- The RDS DB instance will host the data for the Public sector client and access can be managed by roles and KMS.
- C3 application instances will require “Read only” access to the RDS instance, which can be managed using access control lists(ACLs).

Scenario 3 – Proposed

Proposed Architecture for a DB instance in a VPC accessed by an EC2 Instance not in a VPC.



- In this scenario, we propose hosting the C3 application in a EC2 instance which is not in an Amazon VPC.

- The C3 EC2 instance will be able to communicate using “ClassicLink”. When we use ClassicLink, C3 application on the EC2 instance will be able to connect to the RDS instance by using endpoint for the DB instance.
- ClassicLink is available at no additional charge.
- Using ClassicLink, we can connect the EC2 instance to a logically isolated database (RDS), where we define the IP address range and control the access control lists(ACLs) to manage network traffic.